Парламентское собрание Союза Беларуси и России

Постоянный Комитет Союзного государства

Оперативно-аналитический центр
при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Полоцкий государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)

ISBN 978-985-531-564-4

ФОРМИРОВАНИЕ ТРАНСГРАНИЧНОГО ПРОСТРАНСТВА ДОВЕРИЯ СОЮЗНОГО ГОСУДАРСТВА

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: КИБЕРНЕТИЧЕСКИЙ ВЗГЛЯД

Д.И. ВЕРЖБАЛОВИЧ

Республиканское производственное унитарное предприятие «Завод точной электромеханики»

Тема информационной безопасности последние годы занимают все большее место в информационном пространстве. Возрастает количество специалистов, занимающихся различными аспектами этой сферы. Растет и развивается рынок услуг и решений, направленных как на конструктивные, так и на деструктивные действия в этой сфере.

Понятие «Информационная безопасность» эволюционирует и развивается особенно быстро. Сегодня в нем выделяют технологический, социально-политический, медицинский, философский и целый ряд других аспектов. В докладе рассматриваются особенности проблематики информационной безопасности с точки зрения кибернетики.

Современную стадию развития цивилизации часто называют «информационное общество», что объясняется бурным ростом роли и места информации во всех сферах человеческой деятельности. А процесс построения такого общества называется информатизацией.

Кроме множества преимуществ информатизация приводит к возникновению новых – информационных, вызовов и угроз. Соответственно, возрастает роль информационной безопасности – как некоторой сферы деятельности общества, направленной на обеспечение защищенности как информации, так и соответствующей инфраструктуры от случайных или преднамеренных воздействий.

Специализированные издания проблемы информационной безопасности рассматривают уже не только с правовой, организационной и технологической точек зрения, но и с социальной, теоретико-методологической, когнитивной, философской и даже – медицинской. Естественно, что при таком разнообразии подходов имеется достаточно большое количество различных трактовок понятия «информационная безопасность».

При этом часто выделяют две составляющих этого понятия: «***защита информации***» и «***защита от информации***».

Под **защитой информации** обычно подразумевается защита некоторого информационного ресурса от попыток нарушить его целостность, достоверность, получить к нему несанкционированный доступ. Это направление рассматривается как задача, решаемая в первую очередь техническими, а также криптографическими, организационными и административными средствами.

Защита от информации предполагает комплекс мероприятий, позволяющий различными способами препятствовать проникновению и распространению неверной, деструктивной, искаженной информации. Этот аспект важен, в первую очередь, для социальных систем, а также для процессов управления, протекающих в сложных системах. И здесь на первый план выдвигаются психологические, социологические, философские аспекты проблемы – равно как и способы реализации этой защиты.

В докладе показано, что общество все больше виртуализируется, пропитывается информационными технологиями, выстраивает радикально новые системы взаимоотношений, технологии управления. Проблемы информационной безопасности начинают приобретать социально-политический характер. Информационные технологии активно используются для формирования общественного мнения, тонко работают с социальными группами и даже – с процессами человеческой психики. Формируют новые «системы ценностей». Реализуют воздействия «в области смысла» – в когнитивной сфере.

Поэтому последние годы информационная безопасность (как состояние некоторой информационной подсистемы общества) становится важнейшим компонентом экономической, финансовой, политической (и даже геополитической) конкурентоспособности общественных образований, выделяется в качестве составной части национальной и общественной безопасности.

Большинство социальных, политических, экономических, технологических и иных процессов, протекающих в обществе, генерируют и потребляют широкий спектр информации. Соответственно, они зависят от качества, актуальности и достоверности этой информации. А эти показатели, в свою очередь, напрямую зависят от того, насколько безопасна информационная подсистема, обеспечивающая требуемый процесс. Поскольку доля информации в основных общественных управленческих процессах велика и имеет тенденцию к возрастанию, все эти процессы можно считать информационными.

Известно, что наука, занимающаяся вопросами общих закономерностей информационных управленческих процессов – кибернетика. За годы своего развития она сформировала мощные научно-методические подходы и аппараты для решения широкого круга управленческих задач и проблем.

В докладе проблема информационной безопасности рассматривается с кибернетической точки зрения.

В экспертном сообществе существует подход, согласно которого *всю* эволюцию живого можно разделить всего на две эры: докибернетическую и кибернетическую (смотри, например, [3]). Этот пример наглядно иллюстрирует «всеобъемлемость» кибернетического подхода.

Управление является важнейшим компонентом любой кибернетической системы, обеспечивающим ее развитие. А управление практически невозможно без так называемой «обратной связи». Известно, что типовая кибернетическая система представляет собой систему с обратной связью (рис.1).

Рис. 1 – Типовая кибернетическая система

Исходя из анализа приведенной схемы в докладе с кибернетической точки зрения обосновывается необходимость **защиты информации**. Действительно, поскольку процессы в такой системе связаны со сбором, транспортировкой и обработкой информации, к ее качеству предъявляются достаточно строгие требования. Если искажаются сигналы в канале прямой связи – объект управления выполняет не те действия, которые от него требуются. Если искажаются сигналы в канале обратной связи – управляющая подсистема по-

лучает неверную информацию о состоянии объекта и принимает неверные решения. В обоих случаях цель *не достигается*. Система функционирует не эффективно, вплоть до проигрыша в конкурентной борьбе!

Очевидно, что необходимо обеспечить качество информации, передаваемой по каналам прямой и обратной связи. В докладе анализируются возможные способы, которые направлены на решение задачи ***защиты информации***.

Для анализа второй составляющей – ***защиты от информации*** – в докладе типовая схема расширяется и детализируется [2]. Расширенная схема показана на рис. 2.

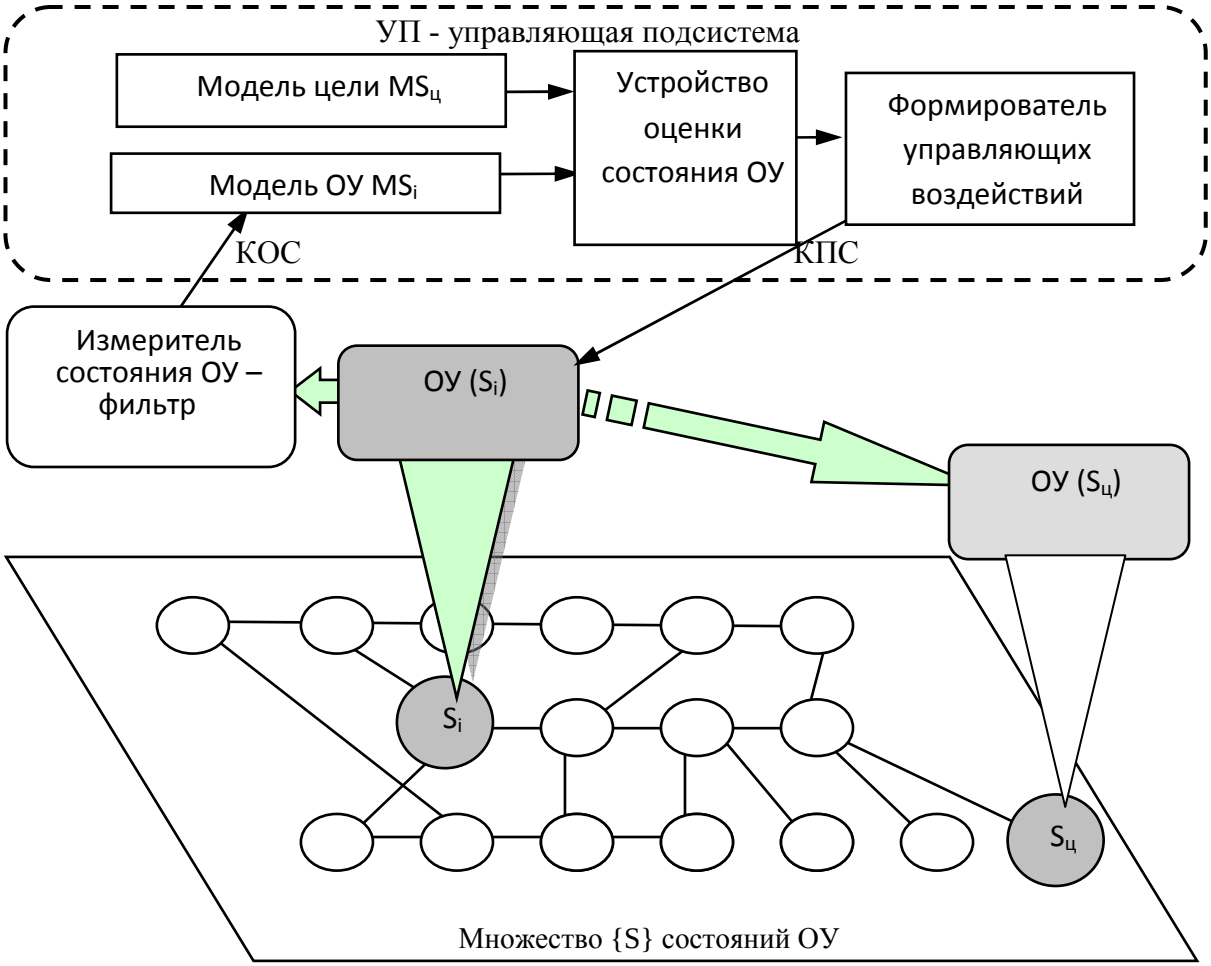

Рис. 2 – Развернутая схема кибернетической системы

В частности, вводится разделение параметров объекта управления на релевантные и нерелевантные. Текущее состояние объекта S_i. = $S(t_i)$ представляет собой совокупность релевантных параметров. Целью функционирования системы будем считать приведение ОУ в состояние $S_ц$.

Для того, чтобы УП вырабатывала правильные управляющие воздействия, она должна обладать сведениями о S_i и $S_ц$. Измеряя различия в параметрах, УП может формировать соответствующие сигналы. При этом S_i определяет измеритель состояния, а вот $S_ц$ должна «присутствовать» в УП заранее. Для этого в УП имеются две модели: модель текущего состояния объекта MS_i и модель цели $MS_ц$. В докладе показывается, что наличие, как минимум, этих двух моделей – есть свойство любой кибернетической системы. Именно с моделями – а не с реальными состояниями – и работает управляющая подсистема. Причем чем сложнее система, тем сложнее модели. Одна из важнейших задач этих моделей – формирование выходных данных, которые поступают на устройство оценки состояния объекта.

Также показано, что в сложных системах, модели формируются в течении длительного времени на основании получаемой информации о внешней среде – идет обучение моделей. Очевидно, что измеритель состояния ОУ должен анализировать и выдавать в УП только релевантные параметры и отбрасывать несущественные. Несущественные параметры могут отрицательно влиять на эффективность функционирования УП (например, растрачивая ресурс УП на их анализ). Поэтому на входе УП должен быть некоторым образом сформирован информационный фильтр, отбрасывающий несущественную информацию и пропускающий релевантную.

Адекватность сформированных в УП моделей играет важнейшую роль в эффективности функционирования сложных систем в целом. Система будет работать неэффективно, если в составе УП будут некачественно сформированные модели. Система либо будет двигаться к неверной цели (если искажена модель цели), либо будет неверно трактовать полученные правильные сведения (если искажена модель состояния ОУ).

С точки зрения кибернетики, система, не обладающая адекватными моделями, обречена на формирование неверных управляющих воздействий и, чаще всего – на совершение ошибок.

Поскольку формирование моделей в сложных системах – процесс длительный (а часто – постоянный), очень важно минимизировать ошибки при их формировании. Очевидно, что информация, ведущая к искажению моделей, представляет для системы угрозу. И тут мы прямо выходим на проблему **защиты от информации**.

В докладе анализируется несколько возможных вариантов отрицательного воздействия некачественной информации на эффективность и устойчивость системы. На взгляд автора, примером формирования неверной модели цели является продвигаемая в мировом масштабе концепция глобального общества. Ведь еще в середине XX века один из основателей кибернетики английский ученый Уильям Росс Эшби открыл закон, который гласит: «*Уровень разнообразия элементов, составляющих систему, определяет уровень ее стабильности. Чем богаче разнообразием своих элементов сложная система, тем она стабильнее. Чем беднее составом система, тем быстрее она распадается от неблагоприятных условий, от любого внешнего воздействия*».

Таким образом, сравнивая проблему защиты информации и защиты от информации можно сделать вывод о том, что последняя способна нанести гораздо больший вред. С другой стороны, сама эта проблема существенно сложнее, генерируемые угрозы многообразнее и «тоньше», Актуальность этой части общей проблемы информационной безопасности заключается в том, что ее последствия могут носить трагический и, даже, катастрофический характер.

Реагирование, предотвращение и нейтрализация угроз в этом случае требует не столько технических, сколько гуманитарных решений, лежащих в областях социологии, политологии, юриспруденции, идеологии и т.д.

Защита от информации актуальна для большинства сложных систем, как технических, так и биологических, и социальных. В докладе высказывается гипотеза, что изучение решений данной проблемы, выработанное такими системами в ходе своего развития, может оказаться полезным для решения проблемы информационной безопасности на современном этапе и в перспективе.

Список литературы

1. Вержбалович, Д. И. Кибервойна. Аспекты безопасности использования информационного пространства / Д. И. Вержбалович. – Мн.: Бел. энциклопедия. – 2015. – 120 с.

2. Колганов, С. К. и др. Особенности компьютерного моделирования в военной сфере / С.К. Колганов, Э.Г. Лазаревич, Д.И. Вержбалович, Ш.Б. Амзеев. – Вопросы оборонной техники. / Науч.-тех. сборник – Серия 3. – 2013 – № 3 (376) – М.: ЦНИИ экономики, информатики и систем управления – С. 11-17.